

**CONTINUATION SHEETS IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations (HSI), of the United States Department of Homeland Security (DHS). I am assigned to the office of the Resident Agent in Charge (RAC) in York, Pennsylvania. I have been employed with HSI since November of 2020. I have successfully completed the Criminal Investigator Training Program and the Homeland Security Investigations Special Agent Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to my employment with HSI, I was employed for four years as a United States Customs and Border Protection Officer at the San Ysidro, California Port of Entry.

2. While employed by HSI, I have investigated many federal criminal violations related to child exploitation, and child sexual abuse material (CSAM). I have gained experience through trainings, both in person and web-based, and everyday work relating to conducting these types of investigations. I have received training in the area of CSAM and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18

U.S.C. § 2256) in all forms of media including computer media.

Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252, and I am authorized by the Attorney General to request and execute a search warrant.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a cellular phone—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

4. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) (Production of

Child Pornography) and 2252 (Possession of Child Pornography), are presently located on the cellular phone described in Attachment A.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is an Apple iPhone 14 Pro Max, further described in Attachment A, hereinafter the “TARGET DEVICE.” The TARGET DEVICE is currently located at the Pennsylvania State Police Barracks at 3800 Black Gap Road, Chambersburg, PA 17202.

6. The applied-for warrant would authorize the forensic examination of the TARGET DEVICE for the purpose of identifying electronically stored data, more particularly described in Attachment B.

PROBABLE CAUSE

7. On or about April of 2024, your Affiant was notified by the Pennsylvania State Police (PSP) that an investigation involving the possession and distribution of illegal controlled substances was being conducted by the PSP Vice Team in Chambersburg, PA.

8. On March 14, 2024, the PSP Vice Team executed a residential search warrant on 658 Heintzelman Avenue in Chambersburg, PA. Two controlled purchases were made at this

residence Present at the residence during the execution of the search warrant was Sean BANKS, Asheyla BARBOUR, and BARBOUR's 4-year-old minor daughter. During the search warrant, the TARGET DEVICE was located in the residence and seized pending further forensic analysis. While the full forensic analysis was being conducted, a partial download of the TARGET DEVICE's contents was made available to the lead trooper on the case, Trooper First Class (TFC) Krista Miller. While examining the partial download of the TARGET DEVICE for evidence pertaining to the narcotics investigation, TFC Miller saw a thumbnail photograph of what appeared to be a prepubescent African American female with an adult erect penis in her hand. TFC Miller was able to access the video that was associated with the thumbnail photograph.

9. The video depicted a prepubescent African American female child, approximately 4 years of age, with an adult erect penis penetrating the child's mouth. TFC Miller was able to identify this child as BARBOUR's 4-year-old daughter who was present at the residence during the residential search warrant executed on March 14.

10. The TARGET DEVICE is currently in storage at the PSP Chambersburg barracks evidence vault. In my training and experience, I know that the TARGET DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the TARGET DEVICE first came into the possession of PSP.

11. Based on my training, experience, and research, I know that the TARGET DEVICE has capabilities that allow it to serve as a storage device for child pornography and as a device for receiving and sending child pornography and communicating with others who have an interest in producing or receiving child pornography. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

12. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically

stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

13. There is probable cause to believe that things that were once stored on the TARGET DEVICE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that data files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a cell phone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a cell phone’s

operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, cell phone storage media contain electronic evidence of how a the device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Cell phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

14. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET DEVICE was used, the purpose of its use, who used it, and

when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the times the cell phone was in use. Cell phone systems can record information about the dates files such as videos and photographs were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a cell phone is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to produce, receive, store or send child pornography, the individual's electronic device will generally serve both as an

instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

15. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises.

Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTOR

16. I know from my training and experience that the following characteristics are prevalent among individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography may collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals may also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their sexual fantasies involving children.

c. The majority of individuals who collect child pornography may often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography may maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often may collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the

Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. However, some individuals may dispose of their collections of their sexually explicit materials or only seek out child pornography when they want to view it, in order to conceal their activities for fear of being caught.

CONCLUSION

17. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the TARGET DEVICE described in Attachment A to seek and seize the items described in Attachment B.

ATTACHMENT A

PROPERTY TO BE SEARCHED

1. The property to be searched is an Apple iPhone 14 Pro Max, hereinafter the “TARGET DEVICE.” The TARGET DEVICE is currently located at the Pennsylvania State Police Barracks at 3800 Black Gap Road, Chambersburg, PA 17202.
2. This warrant authorizes the forensic examination of the TARGET DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

All information and data constituting contraband or fruits, evidence, or instrumentalities of violations of 18 U.S.C. Sections 2251 (Production of Child Pornography), 2252 (Receipt, Possession, and Distribution of Child Pornography):

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, including those in opened or unopened e-mails or text messages. These include both originals and copies.
2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, Internet history, photographs, and any other electronic data or other memory features contained in the device, or SIM card including correspondence, records, opened or unopened e-mails, text messages, chat logs, and Internet history, pertaining to the production, possession, receipt, access to or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or

pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession or production of any child pornography possessed.

3. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or efforts to meet a minor.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of the device or devices associated with the previously mentioned offenses,

including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the device.

7. Documents and records regarding the ownership and/or possession of the searched items.

8. During the course of the search, photographs of the devices may also be taken to record the condition thereof and/or the location of items therein.

9. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

10. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the

device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the device at the time any visual depictions described in paragraph 1 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.